REMARKS

In response to the Office Action mailed November 21, 2003, Applicants respectfully request reconsideration. To further the prosecution of this application, applicants have added claims 22 and 23, canceled claims 1, 2, 3, 6, 15, and 16, amended claims 4, 5, 7, 8, 9, 10, 13, 14, 17, 18, and 19, and amended the specification. Currently claims 4, 5, 7-14, and 17-23 remain pending, of which claims 22 and 23 are independent claims.

Applicants note that the Office Action indicated that Applicants' PTO-1499 from the Information Disclosure Statement (IDS) filed July 5, 2002, was an attachment. The PTO-1449, however, was not enclosed with the Office Action. Applicants respectfully request a copy of the initialed PTO-1449 in the next correspondence from the Office.

On page 2 of the Office Action, several informalities in the specification and claims were objected to by the Office. Applicants, by amendment, have corrected these informalities.

On pages 2-10 of the Office Action, all claims were rejected over combinations of the primary reference Barrett (US Patent 5,199,069) alone or in combination with Masuda (Publication No. US 2003/0046564 A1), Rogaway (US Patent 5,491,749), Blaze (US Patent 5,721,777), and/or Ostermann (US Patent 4,484,025). Applicants respectfully request that these rejections be withdrawn as the amended claims patentably distinguish over these references.

Independent claim 22 recites all of the limitations of canceled claim 1 and further recites: (1) said cryptographic algorithm storage section storing an encrypted cryptographic algorithm; (2) cryptographic algorithm decryption means for decrypting the encrypted cryptographic algorithm; (3) said key information storage section storing a

key for an encrypted algorithm used to decrypt an encrypted cryptographic algorithm as well as the key for cryptographic communication; and (4) key information decryption means for decrypting an encrypted key from said key information storage section.

Applicants note that items (1) and (2) above are limitations formerly present in canceled claim 2, which the Office rejected as being obvious in view of Barrett and Masuda. Barrett and Masuda, however, do not disclose or suggest these limitations, i.e., a cryptographic communication terminal that includes a cryptographic algorithm storage section storing an encrypted cryptographic algorithm, and cryptographic algorithm decryption means for decrypting the encrypted cryptographic algorithm.

The Office acknowledges that Barrett does not disclose or suggest the use of an encrypted cryptographic algorithm. (See Office Action at 4.) The Office thus relies on Masuda to obviate limitations (1) and (2). In Fig. 6, Masuda discloses a drive unit 12, separate from PC 11, that stores an encrypted algorithm. The PC that includes decrypting unit 23 does not include a cryptographic algorithm storage section storing an encrypted cryptographic algorithm, as recited in claim 22. Further, Masuda, in order to use the encrypted algorithm stored in the drive unit, sends the encrypted algorithm over network 32 to server 33, which decrypts and sends the decrypted algorithm back to PC 11. (See Masuda at ¶ 46.) Accordingly, PC 11 of Masuda also does not include a cryptographic algorithm decryption means for decrypting the encrypted cryptographic algorithm, as recited in claim 22, the function of which is performed external to PC 11 by remote server 33.

Applicants further note that the system taught by Masuda represents a significant teaching away from Applicants' invention in that a decrypted algorithm is sent over

network 32 which compromises the security of the algorithm. This is a significant departure from Applicants' invention which recites that the algorithm decryption is part of the communication terminal and therefore not exposed to an unsecure network -- a disadvantage of the prior art pointed out in Applicants' specification: "In updating the cryptographic scheme through the network, however, a problem is posed in terms of safety. For example, confidential information may leak to the outside." (See Applicants' Specification at 2-3.) Thus, because Masuda teaches away from Applicants' invention, it is inappropriate to use Masuda in an obviousness rejection against claim 22. See In re Beard, 16 F.3d 380, 382 (Fed. Cir. 1994) (Board rejection reversed where reference "appear[ed] to teach away from" the invention).

None of Blaze, Rogaway, or Ostermann add to Barrett and Masuda in this respect, as they do not disclose or suggest an encrypted cryptographic algorithm or a cryptographic algorithm decryption means in a terminal, as recited in claim 22.

With respect to items (3) and (4) above, the foregoing references also do not disclose or suggest, in the context of a single communication terminal, a key information storage section and a key information decryption means as recited in claim 22.

Accordingly, it is respectfully submitted that claim 22 patentably distinguishes over the foregoing references and should be allowed. Claims 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 20, and 21 depend from claim 22 and are allowable for at least the same reasons.

Claim 23 includes all the limitations of previous claim 15 and further recites, similar to claim 22, that said cryptographic algorithm storage section further comprises a program for storing an encrypted cryptographic algorithm, and implementing

cryptographic algorithm decryption means for decrypting the encrypted algorithm by using a key for the encrypted algorithm. For similar reasons stated above with respect to claim 22, neither Barrett nor Masuda, nor any of the other cited references, disclose or suggest a computer readable medium that stores a program that implements cryptographic algorithm decryption means as well as encryption decryption means for decrypting received encryption information by using the cryptographic algorithm.

Accordingly, it is respectfully submitted that claim 23 also patentably distinguishes over the foregoing references and should be allowed. Claims 17, 18, and 19 depend from claim 23 and are allowable for at least the same reasons.

In view of the foregoing amendments and remarks, Applicants respectfully request reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: March 22, 2004

By: _____
Christopher S. Schultz
Reg. No. 37,929